REMARKS:

Claims 105, 107, 109-115, 117-118, 127-156, 159 and 162-166 were pending in the application. Claims 105, 107, 115, 118, 127, 128, 135, 136, 143, 148, 152, 155, 159, 162 and 164 have been amended. Claims 168-185 have been added. Therefore, claims 105, 107, 109-115, 117-118 127-156, 159, 162-166 and 168-185 are now pending in this application.

Claim 105

The Examiner rejected independent claim 105 based on a proposed combination of Kouznetsov (U.S. Patent No. 6,973,577) and Chess (U.S. Patent No. 6,772,346). Applicant respectfully disagrees with these rejections.

The Office Action could arguably be read to assert that the static analyzer 52 and dynamic analyzer 53 of Kouznetsov correspond to claim 105's "first plurality of detection routines" and "second plurality of detection routines," respectively. *See* Office Action at 2. As explained in Applicant's Response to Office Action dated September 21, 2007, however, Kouznetsov's analyzers 52 and 53 are both concerned only with what Kouznetsove calls "suspicious" events. *See* Kouznetsov 4:59-5:3. Accordingly, nothing in Kouznetsov can be said to correspond to "first plurality of detection routines" recited in claim 105.[1]

Still further, however, note that claim 105 recites "executing each of a first and a second plurality of detection routines" to obtain first and second scores, respectively. Claim 105 further recites that "upon completing the executing of the first and second plurality of detection routines," the first and/or second scores are used to "categorize the code under investigation." This sequence of events is neither taught or suggested by Kouznetsov, which can be considered to have an "event"-based approach to malicious code detection (Kouznetsov's analyzer 19 waits for system calls to be made by the code under investigation, and then intercepts/analyzes such

[1] Applicant further submits that it is not clear whether programs under test in Kouznetsov (e.g., applications 33, 34 and 35) are "running on an operating system of the computer system," given that monitor/analyzer "functions as a logical 'shim' interposed between the operating system 32 and each of the applications 33, 34, and 35." Kouznetsov at 4:15-25.

calls).[2] In contrast, the method of claim 105 selects an active program, executes each of the recited first and second plurality of detections routines, and, upon completion, categorizes the code under investigation using results of the executed detection routines.

Chess is also cited by the Examiner at pages 3-4 of the present Office Action. As an initial matter, Chess is not directed to analysis of an "active program" as in claim 105; rather, the reference is merely concerned with checking of a "file [that] arrives at a node." *See* Chess at 6:7-8. While Chess teaches checking the file against known non-malicious and malicious files in steps 320 and 340, respectively, *id.* at 6:8-21, this disclosure does not constitute "applying *each* of the first *plurality* of detection routines to the code under investigation to obtain a corresponding one of a first plurality of results" and "applying *each* of the second *plurality* of detection routines to the code under investigation to obtain a corresponding one of a second plurality of results" as in claim 105. Stated another way, claim 105 refers to both a "first plurality of results [i.e., at least two results]" and a "second plurality of results [i.e., at least two results]." Chess does not teach or suggest these features. Chess appears to have a single routine (exemplified by Fig. 3) that checks databases 210 and 220—Chess therefore cannot be said to have a first or second *plurality* of results as recited in claim 105. Chess certainly includes no teaching regarding "weighting" of the "first" and "second" pluralities of results as recited in claim 105.

Accordingly, Applicant submits that neither Kouznetsov nor Chess teaches the "first" or "second" plurality of detection routines of claim 105. Accordingly, even if there were motivation to combine these references in the manner suggested by the Examiner (which Applicant in no way concedes), the resultant combination would not include each and every limitation of claim 105. Accordingly, the proposed combination of Kouznetsov and Chess cannot be used to establish a *prima facie* case of obviousness with respect to claim 105. *See* MPEP § 2143.03. Further, Applicant respectfully submits that the Examiner has not adequately explained why one of ordinary skill in the art would be motivated to modify Kouznetsov in view of Chess, or what such a modification would look like.

[2] Because Kouznetsov utilizes an event-based approach, there is no "selecting" of "an active program as code under investigation," followed by "applying" each of the first and second pluralities of detection routines to the code under investigation, as in claim 105.

For at least the reasons stated above, Applicant submits that claim 105 is patentably distinct over the cited references. Claim 105's dependent claims are patentably distinct over the cited references at least by virtue of their dependency on claim 105. Independent claims 115, 127, 128, 152, and 159 are believed to be patentably distinct (along with their respective dependent claims) for at least reasons similar to those provided above in support of claim 105.

Applicant therefore respectfully requests removal of the § 103 rejections.

CONCLUSION:

Applicants submit the application is in condition for allowance, and an early notice to that effect is requested.

If any extension of time (under 37 C.F.R. § 1.136) is necessary to prevent the above-referenced application from becoming abandoned, Applicant hereby petitions for such extension.

The Commissioner is authorized to charge any fees that may be required, or credit any overpayment, to Meyertons, Hood, Kivlin, Kowert & Goetzel, P.C. Deposit Account No. 501505/6002-00602/DMM.

Respectfully submitted,

Date: December 16, 2008

By: /Dean M. Munyon/
Dean M. Munyon
Reg. No. 42,914

Meyertons, Hood, Kivlin, Kowert & Goetzel, P.C.
P. O. Box 398
Austin, Texas 78767
(512) 853-8847